totalsecurity™

Check Point® SOFTWARE TECHNOLOGIES LTD.

Check Point IPS Engine Architecture:

New Technologies Provide a
Robust Integrated Intrusion Prevention System

Contents

Executive Summary

Some organizations have a love-hate relationship with Intrusion Prevention System technology, and its older cousin, the Intrusion Detection System. On the one hand, IPS is vital for protecting against a deluge of application layer exploits. According to a Verizon Business Report in 2008 hacking led to data breaches by a margin of almost two to one. 39% of the the attacks targeting the Application Service Layer led to data compromise.[1] These attacks often evade usual port/protocol defenses established by a firewall, so detection requires deep-packet inspection with IPS. But when an organization uses in-line blocking deployment of IPS, too often the processing requirements prevent simultaneous use of other security functions.

The dilemma of connectivity or security is now moot. The Open Performance Architecture technology from Check Point will allow implementing as much integrated IPS functionality as required without system degradation. With the Security Gateway R70, organizations can now get fully-integrated IPS with new performance technologies infused in a next-generation inspection engine.

Check Point is the first to exploit performance capabilities of industry standard multi-core processors for IPS. With the Security Gateway R70, intelligent load-balancing among cores enables fast, fully-integrated IPS functions into the industry's leading firewall. This white paper describes how technologies in the new engine fulfill key user requirements. With Check Point IPS technologies, you can have confidence that your organization's network will get top performance and full functionality without compromising on security.

Key IPS Requirements

A suite of Check Point technologies are meeting the rigorous requirements for robust in-line deployment of integrated IPS in the Security Gateway R70. Seven key operational requirements of an IPS system are described below.

Secure — **The IPS's first task is to block attacks coming to your network. Some are known tools and techniques, some are unknown. The IPS should be able to prevent attacks on day 0, so that you can be sure your assets are safe.**

An important requirement for security is elimination of false negatives. This is an event that slipped by undetected is potentially worse than any false positive. Achieving this requires an IPS engine that has multiple methods of detecting both known and unknown threats. Having signatures available that protect against known vulnerability attacks is essential. A good IPS solution will also have zero-day threat prevention to protect against attacks which exploit unknown or undisclosed vulnerabilities. Some methods for detecting zero-day attacks are malicious code detection, detecting anomalous behavior, detection of protocol anomalies, detecting command injection attacks that use html, sql, and ldap, and also detecting phishing attacks.

Fast Performance — **even with extra security functions turned on**

The IPS solution must be fast no matter how you may have enabled security intensive functions in the integrated solution.

[1] Verizon Business Risk Team 2008 Data Breach Investigations Report.

Accurate — minimizes false positives

Distinguishing false positives is essential. A false positive is an event identified as an attack when in fact there is no attack. Too many false positives can cause the administrator to either disable protections or overlook real security issues hidden among volumes of irrelevant or non-important events.

Reliable — maintain systems connectivity and performance for high SLAs

A big obstacle in moving from passive IDS to IPS is that many systems incur network outages, application downtime, and/or performance problems. The solution must be predictable enough so that your organization can try the system in passive mode, and tune it for prevention with predictable results. The solution must also ensure that connectivity is maintained under all scenarios.

Updatable — continuously receives and applies the most recent signatures

The IPS solution must continually evolve so that it can identify changing genres of attacks. A common practice among malware authors is to test their attack against popular anti-malware solutions and modify the attack signature slightly to prevent detection. Lately these attacks have been timed to target systems vulnerable before administrators can apply the monthly Microsoft security update. An IPS solution must provide near real-time threat protection updates to give administrators time to patch vulnerable systems.

Application Aware — enforces policy for applications like P2P and IM

Some peer to peer applications use valuable network bandwidth and create unauthorized paths for the transfer of company confidential data. IPS solutions can play a key role in enforcing company policy for all applications, particularly IM and P2P.

Granular Control — ability to apply only the controls that are necessary, with integrated forensic tools for post-mortem analysis

Other key requirements are setting network exceptions to eliminate inspection of traffic from known safe sources like vulnerability scanning tools, and having forensic tools to aid in the investigation when an attack occurs.

These seven key operational requirements are cornerstones of a high performance and fully functional IPS solution. The remaining sections of this paper describe the details of the different IPS technologies and components in the Check Security Gateway along with the benefits that each component provides to fulfill these seven key requirements.

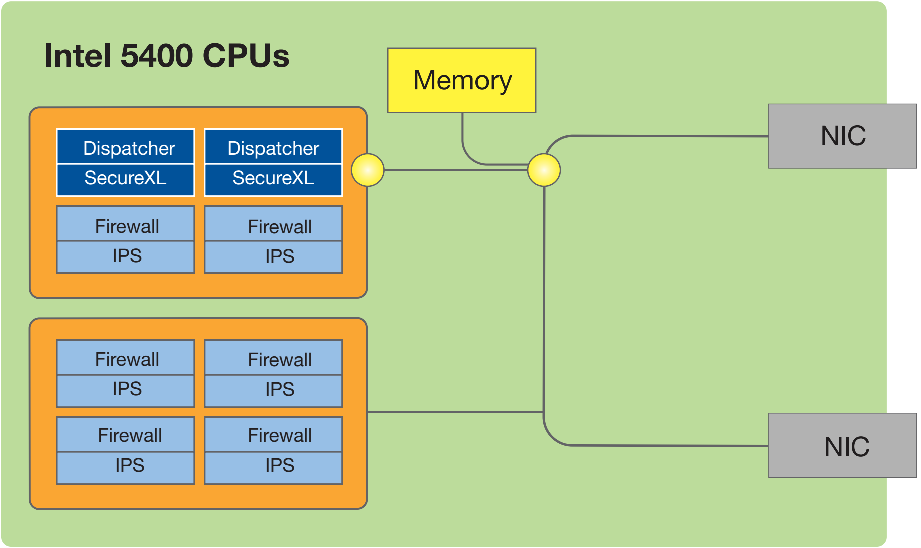
Check Point IPS Technologies

Performance — Accelerated Integrated IPS

When a packet reaches the R70 Security Gateway, the firewall checks the security policy to see if the connection is allowed. If allowed, the packet is accelerated and the connection is offloaded from the firewall to the SecureXL device. SecureXL is a software package with an API for the acceleration for multiple, intensive security operations, including operations that are carried out by a Stateful Inspection firewall from Check Point. Through the SecureXL API, the firewall can offload the handling of those operations to a special module, the "SecureXL device." SecureXL can be implemented at both the hardware layer using network processors, as is done on some “Secured by Check Point” partner appliances, or at a virtualized software layer on open servers.

In a multi-core system, one or more cores perform SecureXL acceleration and also act as a director to distribute the traffic equally to firewall and IPS instances running on the remaining cores. For example, if an appliance contains two quad-core processors, two cores will perform SecureXL acceleration and direct traffic to the other six cores that run firewall and IPS instances.

CoreXL is the first security technology to fully leverage general-purpose multi-core processors. It introduces advanced load balancing to boost throughput for the deep inspection required to achieve integrated IPS on the firewall. When CoreXL technology is activated, it immediately assigns one or more cores that are performing SecureXL acceleration to also act as directors for traffic. The other cores are designated to run instances of IPS and firewall on each core.



Multi-core CPUs Enable Dedicated Processing for Integrated IPS

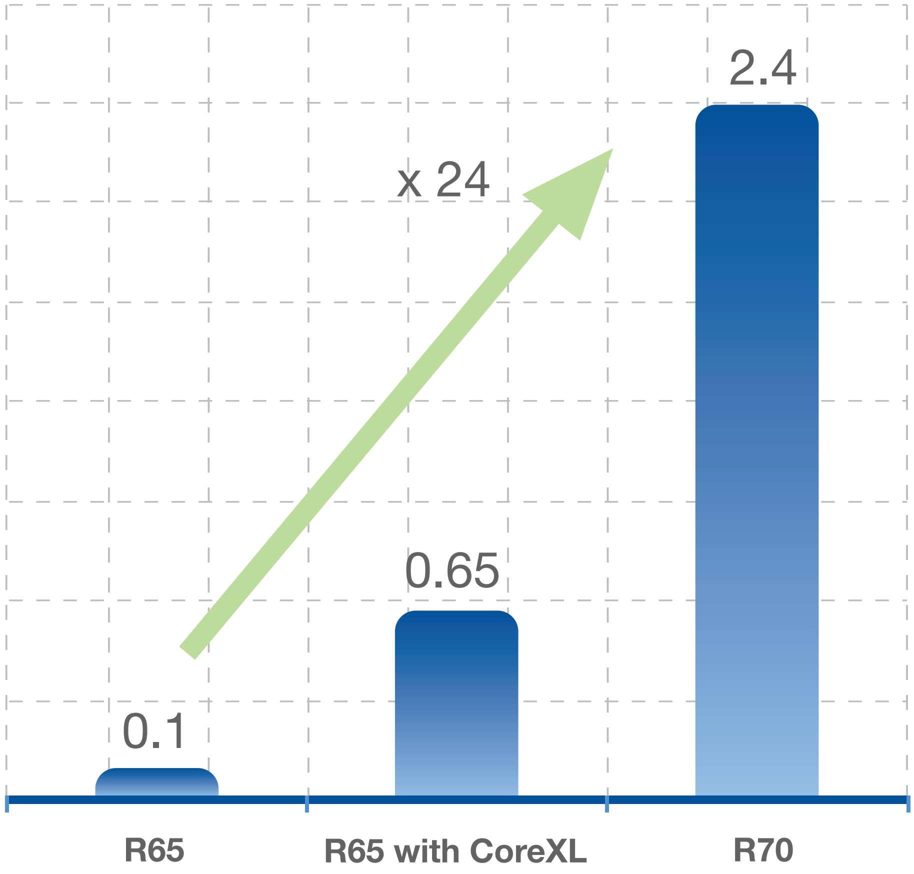
Performance Enhances IPS Detection Engine

Patented technologies underpin a new level of performance for integrated IPS:

- ClusterXL
- SecureXL
- CoreXL

Learn more about how these technologies turbo-charge the Check Point Security Gateway R70 detection engine in a companion paper, Solving the Performance Hurdle for Integrated IPS.

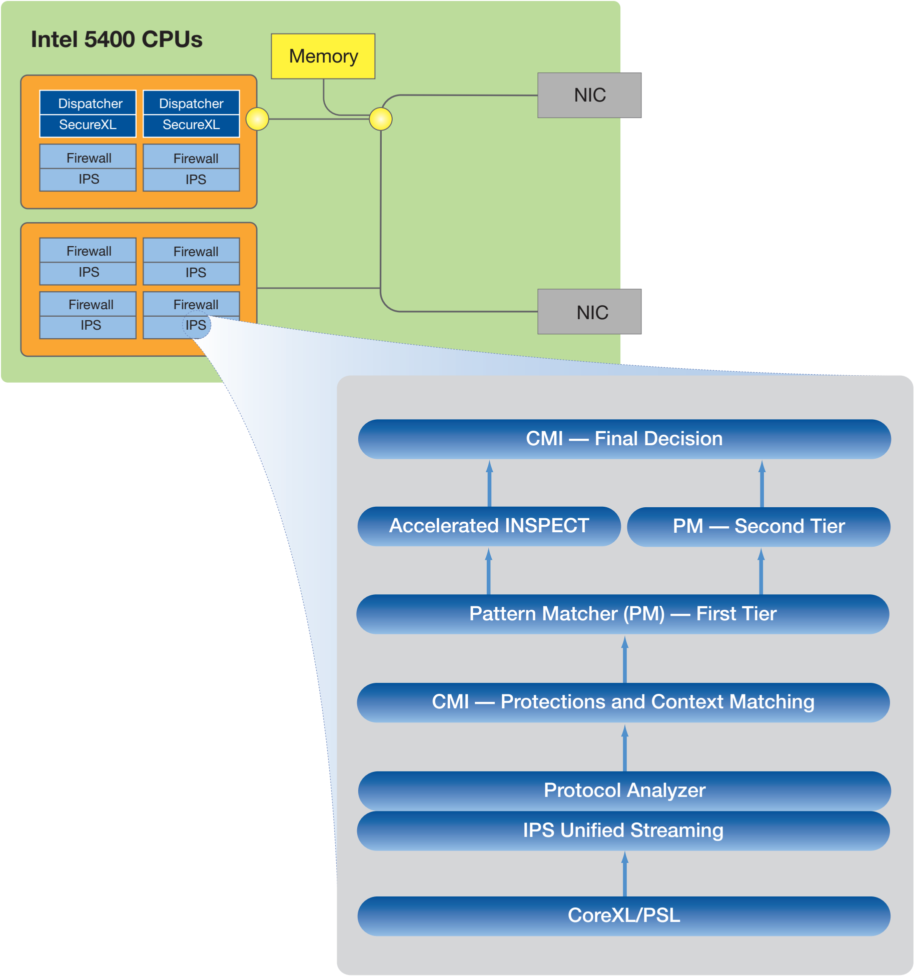
When run on a multi-core processor, the Check Point Security Gateway R70 provides near linear scalability (>70%) per additional core. Throughput performance of the IPS engine can increase an average of 600% with CoreXL activation. In one test, IPS throughput rose from 100 Mbps to more than 2.4 Gbps. Testing parameters were a strict protection profile with 80% of IPS settings activated. Network traffic passed through the gateway represented a blend of protocols and applications similar to that found on the Internet.



IPS Recommended Profile, Traffic Blend Throughput (Gbps)

Secure — Multi-threat Detection Engine

Security Gateway R70 employs a high-speed pattern matching engine to identify attacks that are known and unknown by looking at the specific contexts where the attack occurs in the packet stream. Pattern matching is done via a two tiered inspection. The first tier quickly filters out about 90% of the malicious traffic. Adding additional signatures on the same protocol has minimal impact on performance. The following sections describe the components of this new IPS engine that achieve this great performance.



Key Components of the R70 Multi-threat Detection Engine

Passive Streaming Library

Packets may arrive out of order or may be legitimate retransmissions of packets that haven't yet received an acknowledgment. In some cases a retransmission may also be a deliberate attempt to evade IPS detection by sending the malicious payload in the retransmission. Security Gateway R70 ensures that only valid packets are allowed to proceed to destinations. It does this with Passive Streaming Library (PSL) technology.

PSL is an infrastructure layer, which provides stream reassembly for TCP connections. This layer handles packet reordering, congestion handling and is responsible for various security aspects of the TCP layer such as handling payload overlaps, some DoS attacks, and others. The PSL layer is capable of receiving packets from the firewall chain and from SecureXL module.

The PSL layer serves as a middleman between the various security applications and the network packets. This layer provides the applications with a coherent stream of data to work with, free of various network problems or attacks. The PSL infrastructure is wrapped with well defined APIs called the Unified Streaming APIs which are used by the applications to register and access streamed data.

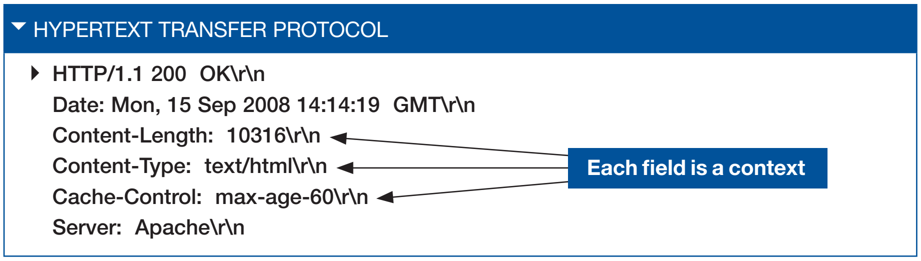
Each application (such as a protocol parser) can register to get streamed data which is relevant to it from the PSL layer. Upon receiving a new connection or new data on an existing connection, the PSL will make sure the packets are in order and continuous data is available since the last application call, and will call the relevant application to handle the new connection or data. When an application decides a packet is malicious, it instructs the PSL layer to terminate the connection.

The PSL layer is also capable of working in a non-streaming mode. In this mode the applications receive the packets of a connection as is without order or retransmission notion. The non-streaming mode is mainly used for applications which wish to inspect UDP connections in which the notion of order or retransmission simply doesn't exist and streaming mode isn't supported.

Protocol Parsers

The Protocol Parsers main functions are to ensure compliance to well-defined protocol standards, detect anomalies if any exist, and assemble the data for further inspection by other components of the IPS engine. They include HTTP, SMTP, DNS, IMAP, Citrix, and many others. In a way, protocol parsers are the heart of the IPS system. They register themselves with the streaming engine (usually PSL), get the streamed data, and dissect the protocol.

The protocol parsers can analyze the protocols on both client to server (C2S) and server to client (S2C) directions. The outcome of the protocol parsers are contexts. A context is a well defined part of the protocol, on which further security analysis can be made. Examples of such contexts are HTTP URL, FTP command, FTP file name, HTTP response, and certain files.



```
▼ HYPERTEXT TRANSFER PROTOCOL
  ▶ HTTP/1.1 200  OK\r\n
    Date: Mon, 15 Sep 2008 14:14:19  GMT\r\n
    Content-Length:  10316\r\n
    Content-Type:  text/html\r\n
    Cache-Control:  max-age-60\r\n
    Server:  Apache\r\n
```

Protocol Parsers Enable IPS Inspection by Dissecting the Protocol for Streamed Data

When the protocol parsers discover a certain context, e.g. the HTTP URL, they will use the next layer, the Context Management Interface layer (CMI) to activate all the protections relevant to this specific context.

In addition, the protocol parsers perform various security checks of their own. These checks are usually validating RFC compliance of protocols and checking for protocol anomalies. Protocol parsers never drop a packet directly. When a protocol parser discovers a vulnerability or anomaly, it notifies the CMI, which then takes the proper action.

Context Management Infrastructure

The Context Management Infrastructure (CMI) is the “brain” of the IPS engine. It coordinates different components, decides which protections should run on a certain packet, decides the final action to be performed on the packet and issues an event log—including a CVE reference if applicable.

Based on the IPS policy, the CMI determines which protections should be activated on every context discovered by a protocol parser. If policy dictates that no protections should run, then the relevant parsers on this traffic are bypassed in order to improve performance and reduce potential false positives. For instance, if the IPS policy is activating server protections only, then the HTTP parser will not analyze the server to client (S2C) traffic.

When a protection is activated, it can decide whether the given packet or context is OK or not. It does not decide what to do with this packet. The CMI is responsible for the final action to be performed on the packet, given several considerations. The considerations include:

- Activation status of the protection (Prevent, Detect, Inactive)
- Exceptions either on traffic or on protection
- Bypass mode status (the software fail open capability)
- Troubleshooting mode status
- Are we protecting the internal network only or all traffic

Pattern Matcher

The Pattern Matcher is a fundamental engine within the new enforcement architecture. It quickly identifies harmless packets, common signatures in malicious packets, and does a second level analysis to reduce false positives. The engine provides the ability to find regular expressions on a stream of data using a two tiered inspection process.

The first tier quickly filters out the vast majority of traffic which is clearly harmless by looking for signatures that are simple to find at a low CPU cost. If the first tier identifies a common attack signature it passes the connection to the second tier to do a second level analysis, thus increasing the confidence that there is indeed an attack. The first tier will never decide on it’s own that a packet is malicious. It can only decide that a packet is clearly harmless. The second tier can also be instructed to activate further inspection using INSPECTv2 technology when some patterns are matched.

Compound Signature Identification

Compound Signature Identification technology does sophisticated signature inspections and application identification. It may match signatures from multiple parts of the traffic in order to identify a malicious activity. CSI can address signatures on multiple parts of a packet, multiple parts of the protocols such as URL and an HTTP header, multiple parts of a connection, such as CIFS request and response, or multiple connections, such as VoIP control and data connections.

In its operation, CSI constructs complex signatures that are triggered only if a certain logical condition over multiple contexts is matched. The logical expression can use AND, OR, NOT or ORDERED-AND to construct the logical expression.

The technique for finding multiple signatures across multiple locations is used to identify complex attacks or P2P applications, and to increase the confidence of simpler protections by looking for more convicting evidence. In some cases CSI is also used to search for patterns across multiple packets and connections without any protocol parsing. An example of CSI use is the CAPICOM protection which looks for one of three signatures. If one is found, then it looks for another signature to validate the finding. Only when all patterns are matched are the protections triggered and the appropriate action taken.

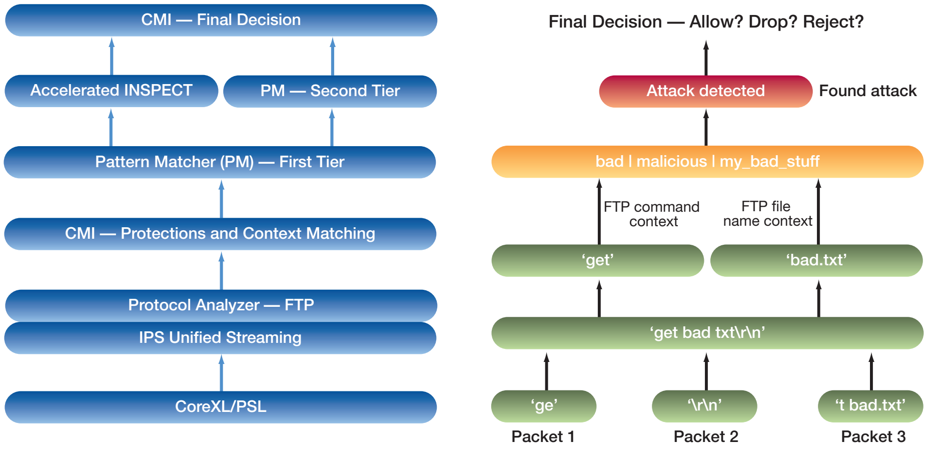
INSPECTv2

In some cases, searching for regular expressions is not enough to identify an attack. In other cases the required regular expression search is expensive in terms of either performance or memory use. Sometimes a calculation is required. The INSPECTv2 engine is used for detection of these complex, elusive attacks. The INSPECT language was one of the cornerstones of the Check Point FireWall-1. Invented in 1993, the INSPECT language provided easy, scalable and an open approach to generic traffic analysis.

INSPECTv2 extends INSPECT to improve performance and increase the ease of writing new protections. It now meets complex parsing requirements needed in a multi-vector attack world. Leveraging concepts from the open N-Code language of Check Point IPS-1, INSPECTv2 offers many programming language tools to easily write new protections such as loops, conditions, states, calculations and others. The improved engine is also accelerated across multiple CoreXL cores. Since the INSPECTv2 engine is more CPU intensive than other inspection layers, it is used only after all other light-weight mechanism's analysis was not conclusive.

How the Architecture Runs IPS

Consider a simple example of an attack and how the IPS engine identifies the attack. Packet Streaming Layer (PSL) technology assembles the streams and passes ordered data to the protocol parsers which parse the traffic to find contexts and protocol compliance anomalies. When contexts are found, then CMI is called to coordinate protections relevant for each context. Each protection can be composed of regular expression matching and INSPECTv2. The regular expression search is usually run first, and then upon matching in both the first and second tiers it calls the INSPECTv2 function that completes the inspection and concludes if there is indeed a match. Once a match is found the flow returns to CMI to decide what to do with the connection based on the IPS policy and which log to send. The diagram below shows the relationships of integrated IPS technologies used in the Security Gateway R70.



Example of How R70 Architecture Inspects Traffic and Identifies Attacks

Check Point IPS Technologies Meets Key IPS Requirements

Consider how the new R70 IPS engine meets the seven key operational requirements of a high performance and fully functional IPS solution.

IPS REQUIREMENT	TECHNOLOGY	BENEFIT
Secure	Passive Streaming Library	Protects against IPS evasion and network attacks
	Protocol Parser	Ensures protocol compliance and anomaly detection
	Pattern Matcher	Quickly identifies common signatures in malicious packets, and does a second level analysis to confirm that the attack is real
	INSPECT v2	Identifies attacks out of well-known contexts, and inspects applications that do not have well-defined protocols
Fast Performance	SecureXL, CoreXL, Medium path IPS acceleration	Flexible and scalable acceleration technology provides performance that adapts to changes in technology and is not significantly impacted when new protections are added. These technologies work together across a wide set of open servers and appliances
	Passive Streaming Library	Works in conjunction with SecureXL to accelerate packets
	Protocol Parser	Protocols are parsed into contexts which allows inspection to be focused on specific parts of the parsed traffic
	Pattern Matcher	A two-tier pattern matching technology that quickly identifies harmless traffic

IPS REQUIREMENT	TECHNOLOGY	BENEFIT
Accurate	Pattern Matcher	Does a second level analysis to confirm that the attack is real
	Context Management Infrastructure	Ensures that the inspection is done only on the relevant content within the protocol, after the traffic is parsed
	Compound Signature Identification	Enables sophisticated signature inspections to identify threats
Reliable	Context Management Infrastructure	Coordinate protection inspection and decide final action
Updatable	R70 IPS Engine	Adding new protections will not degrade performance. Facilitates a quick release of protections from Check Point's global Security Research and Response team which provides customers with industry-leading threat protection response times.
Application Aware	R70 IPS Engine	Application identification enables application policy enforcement. WIth the application awareness, P2P and IM applications, among others, can be simply identified and blocked.
Granular Control	Passive Streaming Library	Provides packet captures
	Context Management Infrastructure	Coordinates IPS policy settings which include activation status, network exceptions settings, and troubleshooting mode status which gives the user exceptional control of their IPS policy

Protect Your Network with Integrated IPS

The Check Point Security Gateway R70 provides the foundation for integrated IPS required by organizations to gain high performance while maintaining a high level of security—all at an affordable price per Gbps of throughput. The Open Performance Architecture of the Security Gateway R70 will help your organization protect its network from evolving application-layer threats, without sacrificing performance or connectivity. Patented technologies underpin performance: ClusterXL, SecureXL, CoreXL, and a new turbocharged IPS engine which will deliver the performance you need to meet all integrated IPS requirements. Check Point, the worldwide leader in securing the Internet, invites you to contact us for more information about Security Gateway R70. To learn more, please contact a Check Point sales representative or visit the Web site at www.checkpoint.com.

totalsecurity™

Check Point®
SOFTWARE TECHNOLOGIES LTD.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Pointsec product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

Worldwide Headquarters
5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: **http://www.checkpoint.com**

May 4, 2009